Financial Management User Group
Meeting Minutes
January 15, 2004

In Attendance

Chief Accountants or Representative:

Shirley Callahan	Preston Ilg	Patricia Schrauben
Mike Draschil	Patricia Lack	Kim Stephen
Joe Frick	Mike Mrazek	Cheri Thompson
Palmer Giron	Melanie Oudsema	Anita Wooton
Rick Harper	Lyle Ross	Deborah Wroubel
Russ Hecko	Lori Schomisch	Penny Wright

All Others:

Cindy Bloomer	Anne Girvin	Cindy Moerdyk
Tracie Briner	Chris Holly	Peggy Murphy
Eileen Bur	Cindy Johnson	Jane Paxton
Marilyn Carey	Jodi Kukla	David Quigley
Dianne Drews	Mary Jo Letner	Doug Ringler
Julie Earle	Dan Lohrmann	Sara Williams
Lisa Fath	Donald Mayes	Arlene Wittenberg
Ronald Foss	Paul McDonald	Rose Zuker
Marge Fuller	Laura Mester	

Opening Remarks

Laura Mester, Chair, opened the meeting at 2:00 p.m. The October 2003 meeting minutes were approved as written. There were no new participants acknowledged.

Laura thanked everyone for a job well done with regard to the 2003 CAFR.

Security Issues

Eileen Bur (Treasury) introduced Dan Lohrmann, the State's Chief Information Security Officer. Mr. Lohrmann discussed the following security topics in a Power Point presentation of security issues that face us in state government (see attachment).

- What's happening in the cyber world
  - Risks
  - Cyber crime is soaring:
    - CD theft
    - Credit card hackers
    - Computer virus
    - Swapping copyright files
    - Bank fraud

- Summary of security issues in Michigan State Government
  - State sees threats daily in:
    - E-mail viruses
    - Scans/probes
    - Web server attacks
    - Computer hi-jack attempts

- Attacking the problem
  - Secure Michigan Initiative

State employees will be asked to take a class in desktop awareness.

The following websites are recommended: www.Staysafeonline.info - online training at no cost; www.nist.gov - National Institute of Standards and Technology. Secure Michigan is using the same guidelines (see attachment for other websites).

The more we can do to standardize our environment and help people understand the issues, the better the financial community will be. Laura questioned if this could cause users to not want to be involved with technology projects that relate to the Internet. Since we have fewer dollars to spend, will we back up and not go forward? Dan responded that the citizens expect to be able to use the Internet for everything while being secure at the same time. A survey was done asking individuals who they trust the most. The number one answer was state government.

If you have questions, feel free to contact Dan Lohrmann at 241-4090 or LohrmannD@Michigan.gov.

DIT Update

Patricia Lack (DMB) reported for Corey Sparks that the planning recommendations for asset management are due mid February. Mike Binkley with desktop has a new automated discovery tool which helps with inventory of personal computers. They are getting the best information they can on desktop counts, and are going to a rated service.

Budget Update

Laura Mester reported that information is available from the Revenue Conference on the Budget website as well as Treasury's website.   The 2005 budget presentation is the week of February 12. Agencies will be impacted in trying to identify expenditure cuts, revenue enhancements, how to stretch the dollar. There may be some pressure for departments to do transfers earlier in the process. The Legislature expects the 2005 budgets should be out by June 11, 2004.

Treasury Update

Eileen Bur reported that check depositing is becoming more risky. Don't assume identify theft is web based only.

Laura noted that we need to make certain the internal control procedures are in place to ensure what we collected or paid is correct.   We need to continue to heighten our awareness; utilize best practices for reconciliations, etc.

The Department of Treasury will be contacting agencies regarding planned disbursement cycles. Treasury is looking at ways to better manage cash.

Eileen thanked those who responded to the survey on credit card accounting and it was determined that CEPAS will not be used for this. The field is a free format field and is not standardized, it would not meet agency needs at a detailed level. The BAI concept may be used which is a file that Treasury gets from the bank. A proposal will be written and reviewed by Treasury and OFM.

Laura said it might help with several types of deposits. If acceptable, we can eliminate agency reclassification entries and essentially do away with the majority of what is in the 4000 fund. It would save processing time and transaction volume. It will be similar to what is done with DI for ICON, Consumers Energy, Detroit Edison, and AEP.

Eileen announced that J.P. Morgan Chase purchased Bank One.

Roundtable Discussion

Imaging payables: Dave Quigley discussed the benefits that can be obtained by implementing a document-imaging program on CD. Benefits include:
- Cost savings in filing reduction
- Faster record retrieval
- Faster communication as images can be e-mailed or faxed
- Reduced printing/copying of images
- Efficient research by program and accounting staff
- Faster audits of records
- Shorter record retention of paper documents at the Record Center

Dave e-mailed agencies after the FMUG meeting inquiring about interest in this program. He shared that the Internet application used by DLEG is a more costly tool than burning the information to a CD, while utilizing the same concept. For more information, contact Brice Sample at Record Retention or Kay Baker, Uday Malavia, Dave Quigley at DMB.

Practices controlling computer equipment: There was discussion among agencies with regard to inventory, physical control issues, computer applications and operations. Laura Mester will talk to DIT's OFM liaison with regard to guidance and procedures on asset management and functionality.

What are the business needs of the agencies as it relates to computer equipment. What is DIT's responsibility related to that and how do we bring it together so it's more manageable and we're not in the middle having discussions on who's responsibility it is.

OFM will facilitate with agencies and DIT on addressing these issues.

Update on number and content of system change requests since PAWS: There are several system enhancement development requests. Some have been distributed to functional owners and are waiting for responses from them. They include:

· Requests related to tracking purchase orders with grant and project numbers.
· Working with Treasury on deletion of multiple errors related to warrants.
· Working with MDOT on their project accounting and ADPICS documents.
· Interface with DCDS called an Enterprise Weekly Activity Reporting System.
· Working with DCH on enhancements to the vendor file and certain mail code, using DCH as a pilot to see if it's possible to batch interface mail code updates.
· We have a DI project with Detroit Edison.

Ways to reduce volume and improve efficiency of interagency transactions: Much discussion and concern from agencies on this issue. Lisa Fath and Tim Becker from OFM will be coordinating a focus group.

Employee reimbursement project: OFM is waiting for Lawson to provide information on this issue. Agencies will be informed at that time.

Systems conversion from NT to XP: Concerns regarding agency systems and interfaces are compatible with the upgrade for MAIN. Laura will be following up with DIT. We need a better form of communication to our agencies relating to this upgrade.

OFM Division Updates

Technical, Audit, and Business Services: Jane Paxton reported that the training and communications area is working on a project to create one OFM Policy and Procedures Manual. It will include accounting, reporting, payroll, and internal controls. This will also include OFM policies in the Administrative Guide and the procedures in the FRAM.

The biennial internal control agency site visits have been completed; the report is in the review process. Overall, statewide evaluations practices have continued to improve. Contact Rick Lowe with any questions.

OFM has developed a security-monitoring guide, which is a checklist to be reviewed and signed off by CFOs and ASA.

The Help Desk is back to a normal volume of calls after the peak period with HRMN Payroll. Please remember to leave a voice mail message when you call so that they can verify the volume of calls not getting through.

There are agency websites that have information about contact and payment express and vendor file information, some information is incorrect. Jane is working with FIA to correct the instructions.   Contact Jane Paxton with any questions at 241-7727 or call the Help Desk.

Financial Operations

Laura reported for Ruth Mealy. The primary focus has been on 1099s and W2s.

Financial Control

Laura mentioned that the 2003 closing was very timely. Issues that came up were dealt with quickly and efficiently. Chief accountants should be proud of their accomplishments. There was a short discussion on year-end overtime and budget issues.

The meeting was adjourned at 4:25 p.m. The next FMUG meeting is scheduled for 2:00 p.m., Thursday, April 22, 2004, in room #3 of the Ottawa Conference Center.

The State of the State for Information Security

Are We in a Cyber War?

Presented by: Dan Lohrmann,

Michigan Chief Information Security Officer

FMUG --   1/14/04

Security Session Agenda

Topic 1: **What's going on around the cyber world?**

Topic 2: **Summary of security issues in Michigan State Government – including recent incidents.**

Topic 3: **How are we attacking the problem in Michigan State Government?**

Technology & Science

HACKS, VIRUSES & SCAMS

Sponsored by **Microsoft TechNet**

News
Business
Sports
Tech · Science
Living
Travel
Health
TV News
Opinions
Weather · Local
Shop@MSNBC
MSN.com

QwestDex
online yellow pages
Find a Local Business

The year the criminals took over

Con artists scam millions in 2002 with help of Internet

By Bob Sullivan
MSNBC

Dec. 31 — This year brought no Melissa virus, no Code Red, no daylong outages at Microsoft or Yahoo, and few tales of high-profile hacks. So one might conclude computer crime was down in 2002. And that would be a mistake. Because this year more than any other, fame-seeking teenage graffiti artists were pushed aside by real criminals who have discovered how user-friendly the Internet is. Millions of dollars are being stolen now from innocent and naive Net users by con artists of every flavor, and there's reason to believe organized crime rings are now taking a sizable slice of that pie. And there's no reason to think things won't get even worse next year.

● E-MAIL THIS ✉   ● COMPLETE STORY ⤵

ADVERTISING ON MSNBC

RESOURCE GUIDE

Hacks, Viruses & Scams

- The year the criminals took over
- Huge ID theft at Pentagon contractor
- High court steps into DVD fight
- Security warning over lottery site

Technology & Science

E-COMMERCE REPORT

Crime Is Soaring in Cyberspace

By BOB TEDESCHI

⊞ Enlarge This

C YBERCRIME, long a painful side effect of the innovations of Internet technology, is reaching new dimensions, security experts say. Spurred by a tightening economy, the increasing riches flowing through cyberspace and the relative ease of such crimes, technically skilled thieves and rank-and-file employees are stealing millions if not billions of dollars a year from businesses in the United States and abroad, according to consultants who track cybercrime.

Advertisement

Thieves are not just diverting cash from

News
Business
Sports
Tech •Science
Living
Travel
Health
TV News
Opinions
Weather • Local
Shop@MSNBC
MSN.com

Why we're all at risk of ID theft

Identity fraud is rampant and protection options limited

D. Hoffmann / MSNBC

ANALYSIS

By Bob Sullivan
MSNBC

Jan. 31 — Carefully guard your Social Security number. Don't enter it in Web pages; don't give it out to companies. Watch your bank statements and credit card bills like a hawk. Shred any

Hacks, Viruses & Scams

- Why we're all at risk of theft
- Bush cyber-security ch resigning
- Phone bill 'cramming' spikes again

USA TODAY.

Money

▪ E-MAIL THIS   ▪ PRINT THIS   ▪ SAVE THIS   ▪ MOST POPULAR   ▪ SUBSCRIBE

Posted 2/18/2003 2:00 PM   Updated 2/18/2003 2:06 PM

Hacker gains access to 5.6 million credit card numbers

NEW YORK (AP) — A computer hacker gained access to more than 5.6 million Visa and MasterCard account numbers by breaching the security of a company that processes transactions for merchants, the card associations said Tuesday.

Visa USA spokesman Mike Riley said that there has been no report of fraudulent activity involving the accounts and that Visa was monitoring the situation.

He said he could not identify the third-party processor or say exactly when or how the hacker got access to the account information, which involves some 3.4 million Visa accounts

RELATED STORIES
Protecting your privacy
• Ring of identity thieves bust

Done   Internet

14-day site search

[ ] **GO**

More search options

Stock Quote

[ ] **GO**

◉ Ticker ○ Name

Intermittent Clouds
H 2 / L -8

More weather

◀ **Previous Story**   ✉ **Mail this story to a friend**   📄 **Printer friendly version**   **Next Story** ▶

Jan. 31, 2003. 05:28 AM

Insurer offers payment to prevent identity theft

Company apologizes for loss of personal data

DANA FLAVELLE
BUSINESS REPORTER

Co-operators Life Insurance Co. says it will compensate customers who incur out-of-pocket expenses in preventing possible identity theft following

Home > Browse Topics > Security > Hacking > Story

U.S. Army Web servers hacked

By DAN VERTON
MARCH 18, 2003

Content Type: **Story**
Source: **Computerworld**

**Security
Knowledge Center**
- Security News
- Discussions
- Events
- Glossary
- Vendor Listing
- Resource Links
- Reviews
- White Papers
- Security XML Feed
- Mobile Channel

WASHINGTON -- Hackers on March 11 infiltrated an undisclosed number of U.S. Army Web servers, taking advantage of a previously undisclosed

File   Edit   View   Favorites   Tools   Help

← Back ▾ → ▾ ⊗ ⟳ ⌂ 🔍Search ☆Favorites 📀Media ⟳ ▾ 🖨 W ▾ 📄 💬

Address http://www.eweek.com/article2/0,3959,1068233,00.asp ▼ ⟳Go Links »
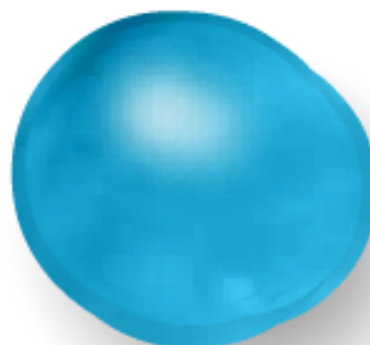
eWEEK

Monday, May 12, 2003

News
eWEEK Labs
Opinion
Rumors
Security
Wireless
Storage
Linux
Company Spotlight
Developer News
Interviews
eWEEK International
Careers Center
Tools & Utilities
IT Infrastructure
Free Subscription
White Papers

Home > **Breaking News** > First Union Hoax on the Loose

May 8, 2003

First Union Hoax on the Loose

By Dennis Fisher

A hoax e-mail purporting to come from First Union Bank and attempting to dupe recipients to visit a malicious Web site is making the rounds on the Internet.

The e-mail arrives from the address bankaccount@firstunion.com and informs the recipient that the bank has lost the recipient's online banking username and password. It directs users to a Web site where they are encouraged to enter their usernames and passwords, which are presumably then collected for later use by the scam artist who created the e-mail.

Bank officials say they're trying to determine who is sending the e-mails.

Even if users don't enter their personal information in the form at the site,

📧 Email th

🖨 Printer-
Version

🖥 Internet

Home > Browse Topics > Security > Story

Viruses get smarter

By DAN VERTON
JANUARY 27, 2003

Content Type: **Story**
Source: **Computerworld**

VPN/SECURITY

Next-Generation Viruses
Read more about the new class of emerging viruses:

▶ Viruses get smarter

10 Tips for Beating Virus Threats

He's been a virus writer for seven years. He goes by the handle Melhacker and may have been responsible for the recent outbreak of the Bugbear worm, the second most prevalent worm on the Internet last year. Now he claims to be working on a new virus, Scezda, that represents a new type of threat.

Scezda, as he describes it, falls into an emerging category of megaworms that combine features from some of this

File   Edit   View   Favorites   Tools   Help

Back

Address   http://www.siliconvalley.com/mld/siliconvalley/6027714.htm

SiliconValley.com

Posted on Fri, Jun. 06, 2003

The Mercury News

Virus sends confidential Stanford information out in e-mail

By Kim Vo
Mercury News

People at Stanford University got some spicy spam Thursday: sensitive information, including highly confidential details about employee salaries and

msn

MID-SIZE HYBRID PRODUCTION VEHICLE.

MSNBC News

MSNBC

News
Business
Sports
Tech • Science
Living
Travel
Health
TV News
Opinions
Weather • Local
Shop@MSNBC

Technology

TECH TOOLS

Sponsored by TOYOTA

House proposal targets file swappers

Bill would make swapping of copyright file a felony

By Declan McCullagh

c|net NEWS.COM

July 17 — Peer-to-peer users who swap copyright files could be in danger of becoming federal felons, under a new proposal backed by Democrats in the U.S. House of Representatives.

File   Edit   View   Favorites   Tools   Help

Back

Address   http://www.washingtonpost.com/wp-dyn/articles/A30330-2003May8.html   Go

TechNews.com   **DAILY TECH E-LETTER** | **ARCHIVES**   SEARCH: News   GO   Search Options

Technology Home

Washtech

Tech Policy

Government IT

Markets

Columnists

Personal Tech

Special Reports

Jobs

washingtonpost.com

More News

Jobs FIND / POST

Cars BUY / SELL

Real Estate BUY / SELL

Microsoft Admits Passport Was Vulnerable

By Ted Bridis
The Associated Press
Thursday, May 8, 2003; 1:02 PM

WASHINGTON - A computer researcher in Pakistan discovered how to breach Microsoft Corp.'s security procedures for its popular Internet Passport service, designed to protect customers visiting some retail Web sites, sending e-mails and in some cases making credit-card purchases.

Microsoft acknowledged the flaw affected all its 200 million Passport accounts but said it fixed the problem early Thursday
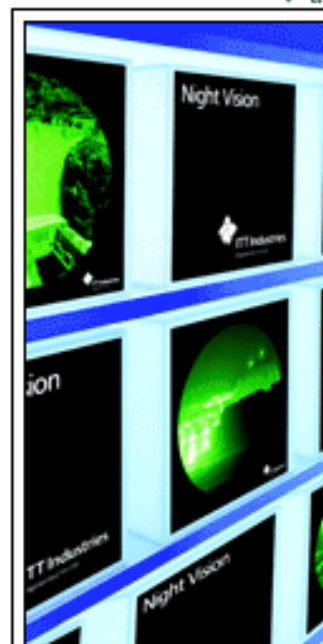
NEWS

Daily News
Vendor News
Newsletter Archives
This Week in print

PRODUCT REVIEWS/INFO

Tests/reviews
Buyer's guides
White papers
Special Reports
Product Central
Webcasts

OPINIONS/FORUMS

Columnists
Forums
Weblogs

RESEARCH CENTERS

HOW TO/PRIMERS

MANAGEMENT/CAREERS

SPECIAL ISSUES

Enterprise Networks / Security /

New worm poses as Microsoft patch

By Paul Roberts
IDG News Service, 07/16/03

Antivirus company TruSecure is warning users about a new e-mail worm that is beginning to spread on the Internet and over the Kazaa peer-to-peer network.

The new worm, dubbed "Gruel" is a mass-mailing worm that masquerades as a Windows software patch from Microsoft and as a virus removal tool from Symantec, according to an alert from TruSecure.

✉ Send

🖨 Print

📄 Feedback

Related links
More on this topic.

Breaking news
Today's top news.

Advertisement:

PRODUCTIVITY   **NETWORK QUIZ**

now

Like other mass mailing worms, Gruel spreads by stealing

File   Edit   View   Favorites   Tools   Help

← Back ▾   → ▾   ⊗   🔄   🏠 | 🔍 Search   ⭐ Favorites   🎬 Media   🌐 | 📋 ▾   🖨   ▦ ▾   📄   💬

Address   🔵 http://www.cnn.com/2003/TECH/internet/07/23/cybercafe.security.ap/index.html

CNN.com./TECHNOLOGY

- Home Page
- World
- U.S.
- Weather
- Business at cnnmoney
- Sports at SI.com
- Politics
- Law
- **Technology**
- Science & Space
- Health
- Entertainment
- Travel
- Education
- Special Reports

Kinko's spy case: Risks of renting PCs

Wednesday, July 23, 2003 Posted: 9:08 AM EDT (1308 GMT)

NEW YORK (AP) -- For more than a year, unbeknownst to people who used Internet terminals at Kinko's stores in New York, Juju Jiang was recording what they typed, paying particular attention to their passwords.

Jiang had secretly installed, in at least 14 Kinko's copy shops, software that logs individual keystrokes. He captured more than 450 user names

File Edit View Favorites Tools Help

← Back ▾ → ▾ ⊗ ⬡ ⬠ | ⊘Search ☆Favorites ⊛Media ⊛ | ⬚▾ ⬚ ⬚ ▾ ⬚ ⬚

CNN.com./TECHNOLOGY

SEARCH

The Web ⦿ CNN.com ○ [   ] **Search** Er

Home Page
World
U.S.
Weather
Business at cnnmoney
Sports at si.com
Politics
Law
Technology
Science & Space
Health
Entertainment
Travel
Education
Special Reports

The New York Times
50% OFF
Home Delivery

SERVICES

adver

Tr
Br
La
Su

Report: Hand-held devices easy to hack

Saturday, August 2, 2003 Posted: 11:55 PM EDT (0355 GMT)

LAS VEGAS, Nevada (Reuters) -- Hand-held computers used to store phone numbers, medical and credit-card information leave millions of gadget lovers fully exposed to identity-theft and other crimes, security experts said Saturday.

Software is now widely available to allow people to steal passwords and other information from popular Palm

TechNews.com   **DAILY TECH E-LETTER** | **ARCHIVES**   SEARCH: [News ▾] [   ]

Technology Home
Washtech
Tech Policy
Government IT
Markets
Columnists
Personal Tech
Special Reports
Jobs
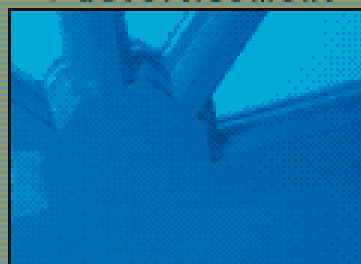
Hacker Gets Acxiom Customer Information

By Caryn Rousseau
Associated Press Writer
Thursday, August 7, 2003; 11:10 PM

LITTLE ROCK, Ark. — A computer hacker gained access to private files at Acxiom Corp., one of the world's largest consumer database companies, and was able to download sensitive information about some customers of the company's clients, the company said Thursday.

METROWEST DAILY NEWS

SEARCH Archives

Enter Keywords GO

Electronic Edition

News & Opinion

Local News

Business
- Boston Business

Opinion
- Dave Granlund
- Mass Hysteria

Obituaries

Columnists

Police / Fire Log

Sports

Arts & Lifestyle

LOCAL NEWS

SEARCH the ARCHIVES

Bank site shut down after hackers attack

Michelle Hillman / News Staff Writer
Sunday, August 24, 2003

NATICK -- The Middlesex Savings Bank was forced to shut down its Web site yesterday after customers complained a hacker was keeping them from doing their banking.

People logging on to the main page of the site

LOCAL REGIONAL

-- RELATED ARTICLES --

The Forces behind Dean

Town likes plan for downtown housing

Retail to play at Loews site in Natick

Water tops

More NATICK Articles

Home   News   Politics   Entertainment   Live Discussions   Photos   Marketplace

TechNews.com   DAILY TECH E-LETTER | ARCHIVES   SEARCH: News ▾

Technology Home
Washtech
Tech Policy
 - Copyright
 - Cybercrime
 - E-Taxes
 - FCC
 - ICANN
 - Security
Government IT
Markets
Columnists
Personal Tech
Special Reports
Jobs
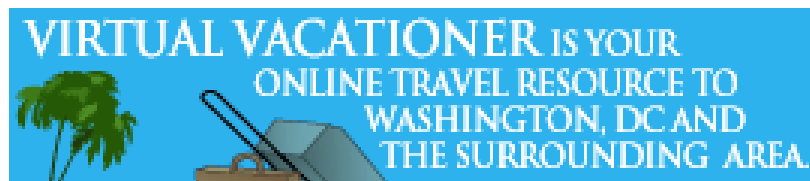
Americans Fear Cyberattacks From Terrorists, Study

By Ellen McCarthy
Washington Post Staff Writer
Wednesday, September 3, 2003; Page E05

Nearly half of all Americans surveyed say they are worried that terrorists could launch attacks through the networks connecting home computers and powerful utilities, a study by the Pew Internet

washingtonpost.com
More News ▾
Jobs FIND / POST
Cars BUY / SELL

File   Edit   View   Favorites   Tools   Help

← Back ▾ → ▾ ⊗ ▣ ⌂ | Search ▩ Favorites ▩ Media ◷ | �▾ ⎙ ▦ ▾ ▤ ◯

Address ▥ http://www.washingtonpost.com/wp-dyn/articles/A12004-2003Sep15.html

TechNews.com

DAILY TECH E-LETTER | **ARCHIVES**

SEARCH: News ▾ [   ]

Technology Home

Washtech

Tech Policy
- Copyright
- Cybercrime
- E-Taxes
- FCC
- ICANN
- Security

Government IT

Markets

Columnists

Personal Tech

Special Reports

Jobs

washingtonpost.com

More News ▾

Jobs FIND / POST
Cars BUY / SELL
Real Estate BUY / SELL

HUMANOLOGY
HUMAN-POWERED TECHNOLOGY

Ga

Companies Scramble to Patch Software Holes
System Administrators Burdened by Number of Vulnerabilities

By Brian Krebs
washingtonpost.com Staff Writer
Monday, September 15, 2003; 7:16 AM

A series of major software security alerts issued by Microsoft Corp. over the past two months is causing headaches for corporate system administrators worldwide.

TORONTO STAR
www.thestar.com

TORONTO STAR

linktotheworld

Tue. Sep. 16, 2003. | Updated at 11:15 PM

| Home | GTA | Business | Waymoresports | A&E |

14-day site search
[ ] GO
More search options

Stock Quote
[ ] GO
⦿ Ticker ○ Name

Sunny
H 25 / L 13
4 Day Forecast

Feature Sections ▾
Today's Features
> Food

> CAREERS
> STAR CLASSIFIEDS
> NEW IN HOMES
> MARKETPLACE

News
Ontario
Canada
World
Opinion/Editorials
Letters
National Report
Obituaries

◀ **Previous Story**   📄 **Print Story**   ✉ **E-mail Story**

Sep. 15, 2003. 11:59 AM

'Error' sends bank files to eBay

Student buys BMO computers, finds client info
Hard drives were on auction

CNN.com./TECHNOLOGY

adver
Yo
Ex
Yo
Do

Survey: Forget work, IM is for flirting, gossip

Tuesday, September 16, 2003 Posted: 11:25 AM EDT (1525 GMT)

LONDON, England (Reuters) -- Flirting with colleagues, scheming against the boss and gossiping about co-workers are among the most common Instant Messenger, or IM, missives circulating around the office, according to a survey released this week.

Instant message

mark303: How are you?
jenny023: I'm fine. How
mark303: Are you doing any
jenny023: I'm not doing anythin
mark303: Oh! wait my boss is
I gotta get off

INDYSTAR.COM

THE ONLINE EDITION OF THE INDIANAPOLIS STAR

MARKETPLACE: **Classifieds • Autos • Apartments • Jobs • Homes • Coupons**   How to adverti
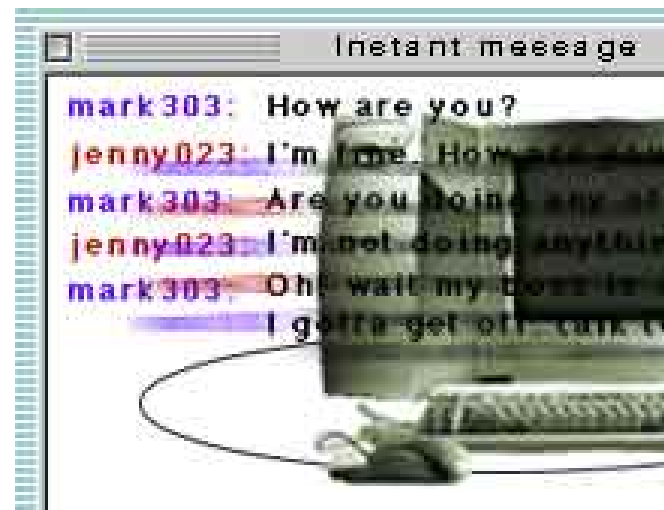
News ▾

City & State

Hamilton County

Star North

Star South

Star West

Obituaries

Commuting

For The Record

Lotteries

Nation/World

Politics/State

Special Reports

30-DAY STORY SEARCH →

SEARCH SPONSORED BY **RE/MAX** THOUSANDS OF HOMES HERE ◀

CITY & STATE

Identity thieves steal $62,000 in casino scam

By Kristina Buchthal
kristina.buchthal@indystar.com
October 8, 2003

It's a casino heist with a high-tech twist -- identity thieves used phony credit cards in a sophisticated scheme to swindle at least $62,000 from five riverboats in northwest Indiana.

The fraud ring, which also struck casinos in Illinois and Nevada, is one of the

Address: http://news.ft.com/servlet/ContentServer?pagename=FT.com/StoryFT/FullStory&c=StoryFT&cid=1059480469585&p=1

FT.com
FINANCIAL TIMES

The world's best business news and analysis in Chinese.

全球经济报道

FINANCIAL TIMES

Chinese.FT.com

Friday Oct 10 2003. All times are London time.

Home US
Asia | Europe | UK
World
Business
Markets
Markets data & tools
Industries
Lex
Comment & analysis
Technology zone
Your money
Arts & Weekend
Sport
Jobs & education
In today's FT
Site services

FT Reports

Home US

Print article | Email

US teen charged with securities fraud

By Adrian Michaels in New York

Published: October 9 2003 16:03 | Last Updated: October 9 2003 19:00

Federal regulators scored another first for the electronic age on Thursday, arresting a 19-year-old living with his parents in Pennsylvania in the first case involving a combination of securities fraud, computer hacking and identity theft.

The alleged behaviour of Van Dinh is a cautionary tale for all internet traders. Officials say he limited his own internet trading losses by tricking another home trader into downloading software, which Mr Dinh then used to steal log-in and password information for an online brokerage account.

Mr Dinh, enforcement officials say, then signed in to the brokerage, buying up most of his own loss-threatening trading positions and saving $37,000. He was arrested on Thursday and charged with fraud by the US Attorney's office in Massachusetts, part of

Search & quotes

[   ]

⊙ News ○ Quotes
• Power search ⓢ
• My portfolio

Editor's choice

The worm that turne on the internet ⓢ

Cisco moves to exp network security business ⓢ

Hollywood's piracy ⓢ

Email & tools

News by email
Personal office

Spy Programs Threaten Data on Personal Computers

By Mike Musgrove
Washington Post Staff Writer
Saturday, October 11, 2003; Page E01

For a computer user, it's the ultimate security headache: A hacker has secretly taken control of the computer and copied sensitive information such as passwords and credit card numbers.

Users often think the odds of getting hit by malicious software are safely low, but there are more invasive and destructive programs on the Web

GCN

Government Computer News | GCN.com

Monday November 10, 2003 | Updated 3:57 PM EST November 10

▼ | Vis

Executive Center   Columnists   Products Central   Site Map   Events   Subscribe

11/07/03

Kansas auditors crack 1,000 passwords

By Wilson P. Dizard III
GCN Staff

The Kansas Health and Environment Department has serious IT security and disaster recovery problems, the state's legislative auditor has found. The auditors said they used password-cracking software to decipher more than 1,000 of the department's passwords— including several administrative passwords—or 60 percent of the total, in three minutes.

The department began fixing the security weaknesses and other problems found in its

Sponsorship Information and

CAUTI

Back   Search   Favorites   Media

Address   http://www.lsj.com/news/capitol/031104idtheft_1a-6a.html   Go   Links

LSJ.com
Lansing State Journal

Detailed forecast >
Sponsored by
BriarWood Realty Co.

Check Your Flight
Airport Information
Bringing Your World Closer

| LSJ.com | News | Sports | Lifestyles | Things to do | Opinions | Classifieds | Searches | Contact Us |

KEYWORD SEARCH

go

MY LSJ

- Subscribe
- Manage my subscription
- Sign up for e-headlines

COLUMNISTS

Andrews: Budget crisis leaves governor few options

Now Gov. Jennifer Granholm is getting ready for another bad-news budget tour. (read more) – Published 10.29.2003

Email this story to a friend | Printable Version

Published November 04, 2003

State bills would offer identity theft protection

Plan aims to help victims, prohibit damage to credit

By Stacey Range
Lansing State Journal

Gordon K. Davis was more than a little confused when he opened his credit card bill last fall.

The Potterville man had never visited the Florida town where charges were made at a dozen gas stations and twice at a movie theater north of Miami.

Now a year since his identity was stolen, Davis finally has his credit

CHRIS HOLMES/Lansing State Journal

washingtontimes.com

Advertise Subscription

Search

- Site Map
- Front Page
- Nation/Politics
- World
- Commentary
- Editorials/Op-Ed
- Metropolitan
- Sports
- Business
- Special Reports
- Technology
- Entertainment

Business

| Nation/Politics | World | Commentary | Classifieds |

ID thefts stifle online buying

By Tim Lemke
THE WASHINGTON TIMES

Many Internet users are considering curbing their online shopping this holiday season for fear of identity theft and spam, but Internet sales still are expected to reach all-time highs.

Online retailers anticipate a 20 percent boost in November and December sales compared with last year, according to Jupiter Research. But beneath those

TOP STORIES

- Terror detainees will be released
- Iraq-al Qaeda link comes in focus
- Seniors medical care poses bias question
- Lincoln's words noted, misquoted
- Blacks 'still claim' Jackson
- Rescue dogs studied for site health risks

File   Edit   View   Favorites   Tools   Help

⇦ Back ▾ ⇨ ▾ ⊗ 🖹 🏠 | 🔍 Search 📑 Favorites 📀 Media 🎨 | 🔛 ▾ 🖨 🗐 ▾ 🗐 💬

Address 🔗 http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,88227,00.html?SKC=cybercrime-8822 ▾ | 🔗 Go | Links »

COMPUTERWORLD
An IDG company

QuickLink [   ] ●   Search [Computerworld ▾] [   ] ●   Advar Se:

| Home | News | **Browse Topics** | Departments | Services | Subscribe | Events | Store | Jobs |

Management   Careers   Security   Hardware   Software   Data Mgmt   Networking   Government   Mobile   Development   Industry

VeriSign

Home > Browse Topics > Security > Cybercrime > Story

Finance sector bracing for upswing in Internet fraud

Cyberscams expected to soar in 2004, experts say

Story by Bernhard Warner

DECEMBER 15, 2003
(REUTERS) - LONDON --
Banking officials and computer
security experts predicted
today that the wave of
cyberscams targeting the
financial services sector will
soar in 2004 as the industry
braces for a new onslaught of
fraud schemes.

The gloomy prediction comes

**Security
Knowledge Center**
- Security News
- Discussions
- Events
- Glossary
- Vendor Listing
- Resource Links
- White Papers
- Security XML Feed
- Mobile Channel
- E-mail newsletters

Knowledge Centers
- Careers
- CRM

LATEST HEADLINES

TOP STORY

- **Demanding a Better Desktop Alternative**
- Sun continues effort to boost IT services unit
- PeopleSoft squeezes out seven cross-portfolio apps

CYBERCRIME NEWS
- Finance sector bracing for upswing in Internet fraud
- Feds Say IT Security Lacking
- Spanish police arrest alleged Raleka worm author

McAfee SECURITY

It means
start

🔗 Done   🌐 Internet

🏁 Start | 📇 🅔 🎯 | 🌐 Novell GroupWise - Mailbox | 🔗 Finance sector bracing... | 🔊 ◀ 🔊 ... 8:37 AM

File   Edit   View   Favorites   Tools   Help

Back   Search   Favorites   Media

Address   http://www.vnunet.com/News/1151553

This week's news [7 day archive]

Analysis

Comment

Forums

Specials

Sign up for a newsletter

Try vnunet.com's Pocket Edition

Mole's commentary on the news

Search News

[   ]   Go!

News areas
⊞ Ebusiness

Xmas virus on the cards

By Roger Howorth [15-12-2003]

Users warned to beware emails bearing .gifs

Security experts last week warned that hackers are preparing Christmas card emails that appear to lead to innocent images, but in fact trick users with Windows systems into downloading viruses.

To avoid difficulties, firms should check their mail filtering

Address http://www.gcn.com/vol1_no1/daily-updates/24475-1.html

Government Computer News | GCN.com

Friday December 19, 2003 | Updated 9:42 AM EST December 19

PostNewsweek Tech Media

Visit our other sites

Executive Center   **Columnists**   **Products Central**   **Site Map**   **Events**   **Subscribe**   **My Account**

Search GCN

Advanced Search

Quickfind | Help

Hot Topics

Biometrics
Defense IT
Enterprise Architecture
E-Government
Homeland Security
IT Infrastructure
IT in Action
Knowledge Management
Mobile & Wireless
New Products / Technology
Outsourcing

12/18/03

Hackers hit NASA Web sites

By Joab Jackson
GCN Staff

Hackers attacked 13 NASA Web sites yesterday and changed their contents, agency spokesman Brian Dunbar confirmed today. As a result of the compromise, the agency has taken the sites offline until the vulnerabilities can be identified and fixed, he said.

All the sites were subdomains of the Nasa.gov Web address, including the NASA Research & Education Network (www.nren.nasa.gov), the Advanced Supercomputing Division (www.nas.nasa.gov), the Information Power Grid (www.ipg.nasa.gov) and the Computing, Information and Communications Technology Program (www.cict.nasa.gov).

Printer-Friendly Version   E-Mail This Article
Purchase A Reprint   Link To This Page

Sponsorship Information and Announcements

GCN MANAGEMENT LEADERSHIP AWARD

Deadline: January 16, 200

Sports
Chats and Forums
Contests/Free Stuff
Community Events
Your Comments
Advertising

Search NBC25

[GO]

NEWS 25

Reeders
Memorial Home
A tradition of compassion, the future of caring in a Christian atmosphere

Frederick County, MD

Police bust million-dollar identity theft ring

✉ Email to a Friend   🖷 Printer Friendly Version

By *Amanda Mallonee*

FREDERICK, MD JANUARY 9- Officials are calling it the largest illegal ID factory bust in the Baltimore- Washington area. The Frederick County Sheriff's Office says a year-long investigation has led to the arrest of a Frederick-area man on identity theft charges.

This entire investigation started when a Michigan man reported someone had stolen his identity and opened accounts at Frederick's Bon-Ton and Sears stores.

Frederick County Sheriff's Office detectives recently identified a suspect in the case as 39-year-old Jian Wang of Frederick. Detectives were following Wang when he was stopped for a traffic violation Wednesday on I-95. A fake name and birthdate on his driver's license prompted officers to search his car and eventually his home.

During those searches, police found fradulent credit cards, social security cards and the equipment to make them. Detectives think Wang was using the illegal credit cards to buy computers, jewelry, furniture, and electronics. At this point, detectives

Related

C 12-Jan @

50.5
50.0
49.5
49.0

Tue   Wed

C   49.85
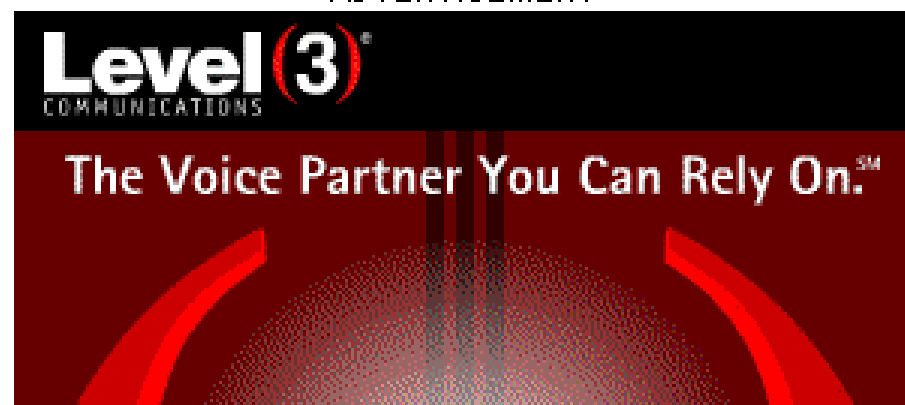
View Deta

Delayed
Quote data prov

Reuters
Citibank warns on new Internet "phishing" scam

Monday January 12, 12:36 pm ET

By Jonathan Stempel

NEW YORK, Jan 12 (Reuters) - Citibank on Monday warned customers not to fall for an e-mail fraud that urges them to log into a bogus Web site to verify that their accounts have not been tampered with.

"It's a scam," said Mark Rodgers, a spokesman for the bank, a unit of Citigroup Inc. (NYSE:C - News) "Consumers have reported receiving fraudulent e-mails that appear to be from Citibank, but which are in fact sent by impostors."

Related Ne
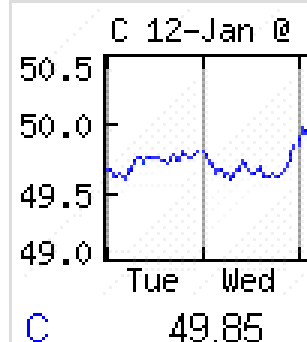
· Standard Life: Share Sale No Solvency - Dow. News (6:36 am)

· Depfa EUR3 B Thursday; Pric +0.10 - Dow Jone (6:14 am)

· Citigroup lawye Parmalat pross

File Edit View Favorites Tools Help

⇐ Back ▾ ⇒ ▾ ⊗ ▣ ⌂ | ◎Search ﹡Favorites ◎Media ◎ | ▤▾ ▤ ▦ ▾ ▤ ◎

Address http://www.washingtonpost.com/wp-dyn/articles/A13587-2004Jan13.html

Microsoft Patches Fail To Fix Dangerous Security Flaw

By Brian Krebs
washingtonpost.com Staff Writer
Tuesday, January 13, 2004; 4:26 PM

Microsoft Corp.'s latest round of software patches fails to fix a flaw in its Internet Explorer Web browser that makes it easier for online criminals to dupe people into disclosing their credit card numbers, passwords and other private data.

Security experts were hoping that the patches, which were released today, would address the problem, but a
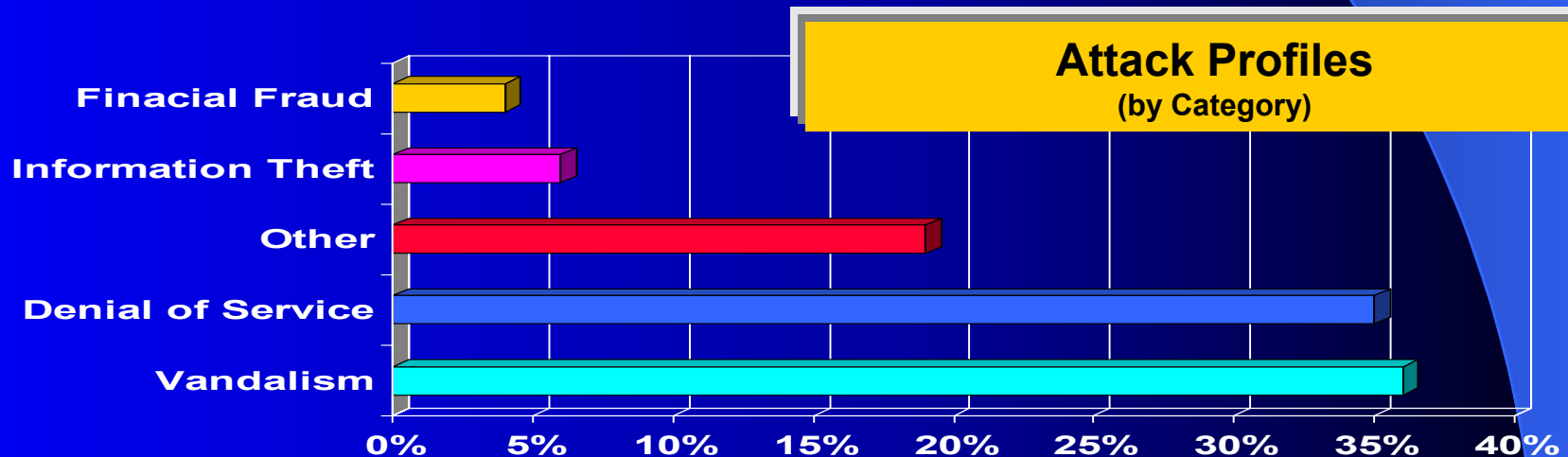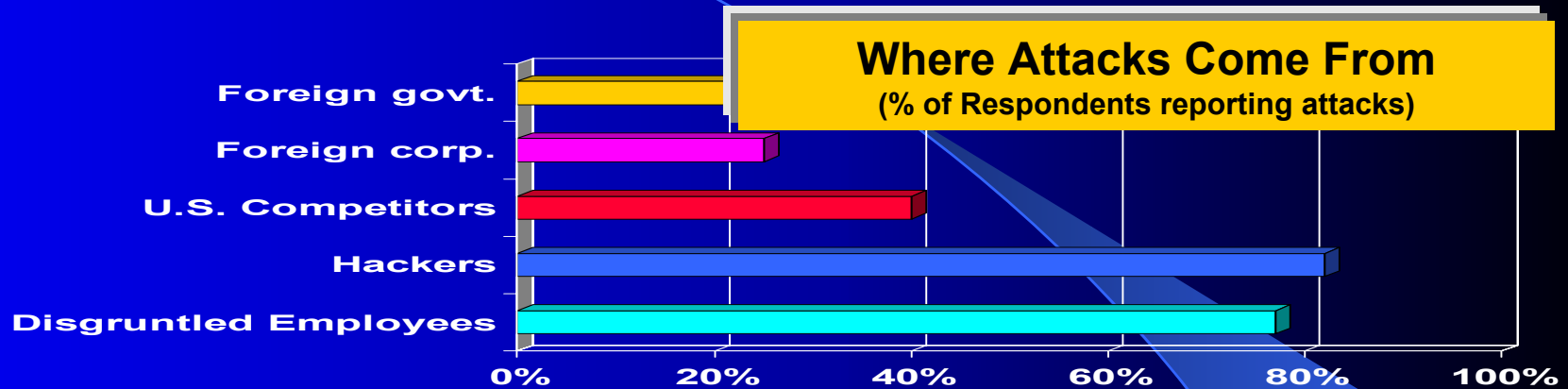
Is Michigan at Risk?

Where Attacks Come From
(% of Respondents reporting attacks)

Foreign govt.
Foreign corp.
U.S. Competitors
Hackers
Disgruntled Employees

0% 20% 40% 60% 80% 100%

Attack Profiles
(by Category)

Finacial Fraud
Information Theft
Other
Denial of Service
Vandalism

0% 5% 10% 15% 20% 25% 30% 35% 40%

Source: 2003 CSI/FBI Crime & Security Survey

State Sees Threats Daily

- Typical Incidents per day (approx.)
  - 1500 e-mail viruses
  - 38,000 scans/probes
  - 620 web server attacks
  - 3 Computer Hi-jack attempts

Typical Incidents and Causes

- Trojan/System Backdoor
  - Acceptable Use Violations:
    - Peer-to-Peer file sharing
    - Instant Messaging (Chat programs)
    - Visiting Inappropriate Sites
    - Online games

- Website Defacements
  - Need for Patch Management
  - Need for Change Management

Typical Incidents and Causes Continued

- Worms/Viruses
  - County network connections (CodeRed.F)
  - Contractors plugging in infected laptops on SOM network (SQLSlammer)
  - Employees dialing into network with unsecured and infected home machines (MS Blaster/Nachi)
  - Peer-to-Peer file sharing (Klez.h, BugBear)

- Illegal/Inappropriate Activity
  - Child pornography
  - Copyright violations (Pirated software, music,movies)
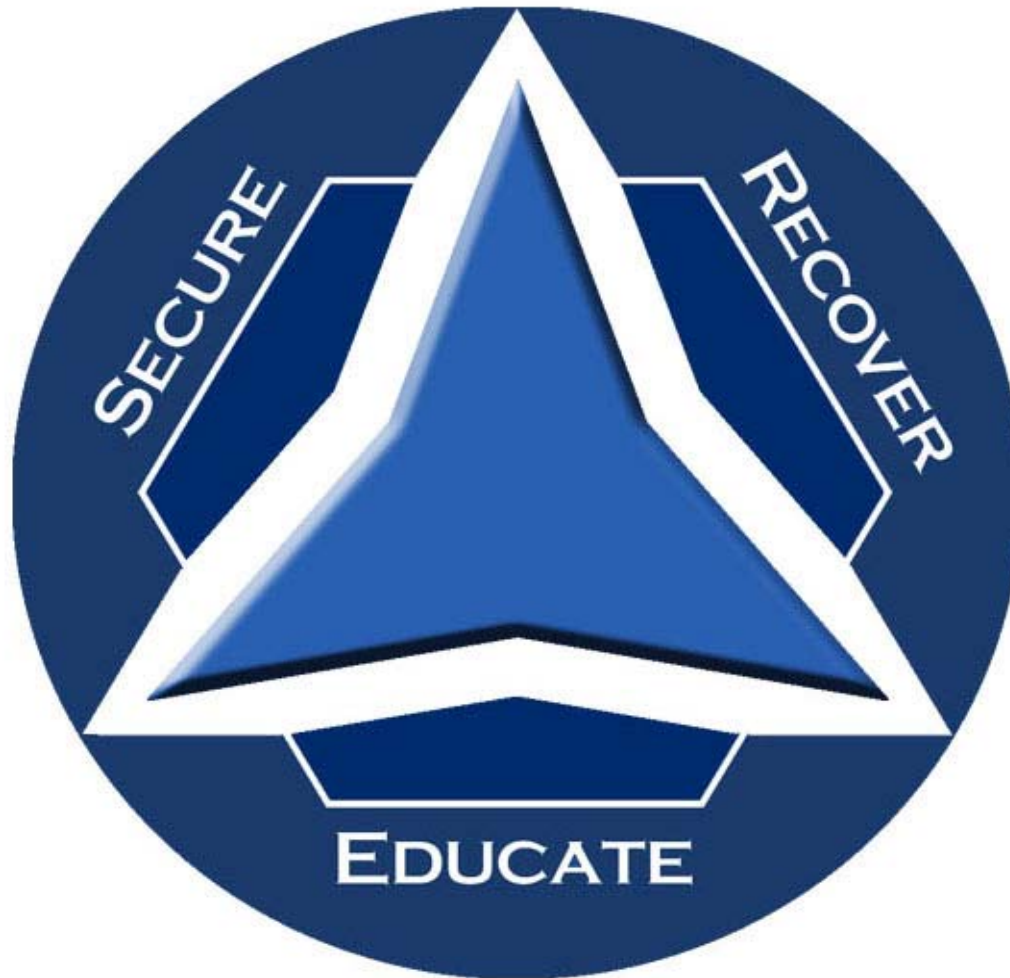 - SPAM

Consider These Questions

- Can I **Detect?**
  - an intrusion as it occurs across my entire network?

- Can I **React?**
  - with sufficient speed and resources to minimize loss?

- Can I **Identify?**
  - what systems and data were compromised?

What is my risk of loss if I can't?
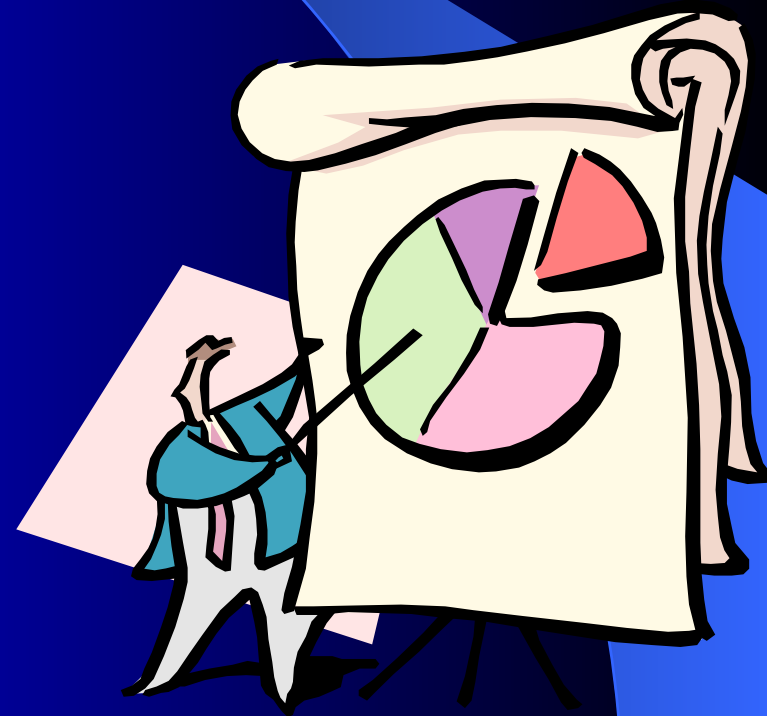
THE SECURE MICHIGAN INITIATIVE

SECURE

RECOVER

EDUCATE

OFFICE OF
ENTERPRISE SECURITY

DEPARTMENT OF INFORMATION TECHNOLOGY

The Process

- Rapid risk assessment

- As is analysis

- Gap determination

- To be Security recommendations

Results

Based upon the DIT rapid risk assessment, the. Enterprise security group had recommendations in the following six(6) focus areas:

1) Roles and responsibilities.
2) Security awareness, training and education.
3) Security incident management.
4) Computer security risk management.
5) Disaster recovery.
6) Certification and accreditation of applications and systems.

Office of Enterprise Security
What Do We Do?

- Michigan IT Strategic & Tactical Security Plans

- Coordinate Incident Response, Patch Management, Security Awareness, Risk Management, DR, and security certification/accreditation processes within DIT

- Homeland Security Liaison, Cyber-Security Committee Chair, Critical Infrastructure Protection (CIP) Co-Chair

- NASCIO & other national + state + local coordination

- DIT Emergency Management Coordinators (DIT EOC)

- MITech Security Sub-Committee, SDII Phase 2 Processes

Where's Help
At Home & Work ?

Michigan State Government Awareness Training is coming

Good Websites: http://www.staysafeonline.com
http://www.staysafeonline.info
http://www.getnetwise.org/
http://www.besafeonline.org

Some Practical Tips -- What can you do?

1. Keep your personal information private including your name, phone number, address, passwords and social security or credit card numbers.

2. Turn off the computer if you feel uncomfortable with what you are seeing on the screen.

3. Never agree to let children meet someone in person who they have met online.

4. Don't share photos of yourself with strangers.

5. Keep the computer your child uses in a central location.

6. Join children as they surf the Internet.

7. Install anti-virus and firewall software on your computer.

8. Remember, not everyone on the Web is who they say they are.

Where's Help?
Public Sector - State/Federal

- **White House** – http://www.whitehouse.gov/homeland

- **Department of Homeland Security** – http://www.dhs.gov

- **Michigan Homeland Security Website** – www.michigan.gov/homeland

- **National Infrastructure Protection Center (NIPC)** – Recently renamed to Information Analysis Infrastructure Protection (IAIP) http://www.nipc.gov

Where's Help?
Public Sector - NIST

National Institute of Standards and Technology

Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurements, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST carries out its mission in four cooperative programs:

Manufacturing Extension Partnership, a nationwide network of local centers offering technical and business assistance to smaller manufacturers; and Advanced Technology Program, which accelerates the development of innovative technologies for broad national benefit by co-funding R&D partnerships with the private sector. http://www.nist.gov/

SP- 800-12- Information Security, The NIST Handbook
http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

SP-800 –18 – Guide For Developing Security Plans
http://csrc.ncsl.nist.gov/publications/nistpubs/800-18/Planguide.PDF

Questions?

Contact Information:

Name: Dan Lohrmann

Phone: (517) 241-4090

e-Mail: LohrmannD@mi.gov